SECURING SENSITIVE CONFIGURATION DATA REMOTELY

ABSTRACT OF THE DISCLOSURE

Personal computer (PC) systems that are remotely managed are equipped with protected storage that is accessible only by Basic Input Output System (BIOS) code. The protected storage has the capacity to store a symmetrical encryption Key. An electronically erasable programmable read only memory (EEPROM) which normally contains the BIOS code is used to store accessible configuration data as well as previously remotely unaccessible sensitive access information (e.g., passwords). The EEPROM is write protected with standard write protect algorithms and access the alterable EEPROM data is through write requests to the BIOS code. Previously remotely unaccessible sensitive data is encrypted with the symmetrical encryption Key by the BIOS code. Remote access to the sensitive data is accomplished via change requests submitted to the BIOS code over a secure channel. The BIOS code has data that allows it to determine if the request is valid. If the request is valid, the sensitive data is decrypted, altered, encrypted, and re-written into the EEPROM. Normal access to accessible data is un-affected and remote access is allowed by validated runtime agents without changing system architecture. Also protected storage is reduced and is its size is not dependent on the amount of secure data in the PC system.

::ODMA\PCDOCS\AUSTIN_1\165766\1
1097:7036-P176US